SERVICE AGREEMENT TEMPLATES FOR “NETLOCK” CLOUD SERVICES

NETLOCK Informatics and Network Security Services Limited Liability Company

CONTENTS

INDIVIDUAL SERVICE AGREEMENT

For the issuance of **Qualified personal signing certificate - RQSCD (VideoRA)**, for rendering related status services as well as for providing and using timestamp, remote key management and signing services

(1) concluded by and between

a\ the Applicant, as the natural person subject of the requested certificate (hereinafter: Client),

b\ and NETLOCK Kft. (registered office: H-1101 Budapest, Expo tér 5–7., tax number: 12201521-2-42, website: netlock.hu), as the qualified Trust Service Provider issuing the requested certificate (hereinafter: TSP)

– jointly referred to as Parties – subject to the following terms and conditions.

(2) The issuance of the requested certificate, the remote management of the signature creation data (private key), the use of it within the framework of remote signature services and the related services shall be governed by the documents titled *Service Policy for qualified certificate services* (hereinafter: Service Policy) and the *Service Practice Statement for qualified certificate services* (Service Practice Statement) prevailing at the time of concluding the agreement.

(3) The rendering and use of the qualification timestamp servic available within the remote signing service specified in the previous paragraph shall be governed by the document titled *Service Practice Statement for qualified timestamp service* prevailing at the time of concluding the agreement.

(4) The business, legal and technical conditions of concluding the agreement are included in the prevailing version of the General Terms and Conditions (hereinafter: GTC) at the time of concluding the contract, available on the TSP’s website.

(5) The TSP makes a statement about its data processing practice in the Privacy Policy published on its website.

(6) For the information necessary for the Relying Parties during the use of the service see: https://netlock.hu/info/#!/relyingparties

(7) The certificate requested by the Client shall be the qualified personal signature certificate within the meaning of Section 1.2.1 of the Service Practice Statement.

(8) Pursuant to Section 1.4 of the Service Practice Statement, the requested certificate and key pair belonging to it may be used subject to the following restrictions:

a\ with the private key belonging to the certificate the Client may create a qualified electronic signature in his own name;

b\ the certificate and the public key belonging to it may be used for establishing the validity and origin – i.e., the identity of the signatory natural person (Client) – of the signatures created by the private key;

c\ the certificate and the key pair belonging to it shall not be used for purposes other than specified above.

(9) In accordance with Section 3.2.1 of the Service Practice Statement, the TSP shall ensure within the framework of the remote key management service that the private key (signature creating data) of the key pair generated for the requested certificate is under the sole control of the Client (in his capacity as the natural person subject of the certificate and as End User) from the moment of its generation until the end of its life cycle.

(10) In accordance with Section 4.1.2 of the Service Practice Statement, Client, as the natural person Subject of the certificate, shall represent as follows:

a\ I have read and accept the GTC, the Service Policy, the Service Practice Statement and the Privacy Policy;

b\ I have read, understand and accept the Client’s obligations specified in paragraph (21);

c\ I shall use my private key (signature creating data) only on the cryptographic device specified in paragraph (15), provided by the TSP;

d\ the subject data specified in paragraph (16) and the other data I have provided during the application for the certificate for the purposes of my identification are true;

e\ I request that the TSP embed my public key generated during the application in the certificate, to certify it and to issue the requested certificate;

f\ I have read and accept the conditions of data processing;

g\ during the validity of the certificate, I shall forthwith inform the TSP of any change in my data stated in the application;

h\ I have read and accept the selected business conditions;

i\ I agree to my obligations under paragraph (21);

j\ my fee payer and invoicing data are correct and true.

(11) Pursuant to Section 4.9 of the Service Practice Statement, Client is entitled to apply for the revocation of her/his certificate as follows:

a\ electronically, identifying her-/himself in TSP’s online system; in this case the revocation takes place immediately after the recording thereof in TSP’s system or within 60 minutes, at the most;

b\ by e-mail in the manner specified on TSP’s website; in this case the TSP shall perform the revocation within 24 hours from the receipt of the revocation request.

(12) In accordance with Section 4.10 of the Service Practice Statement, the TSP shall provide the related certificate status services (CRL, OCSP) from the issuance of the requested certificate by the end of its validity specified in paragraph (19).

(13) In accordance with Section 4.11 of the Service Practice Statement this agreement

a\ is concluded for a definite period, for the full validity period of the certificate specified in paragraph (19);

b\ shall not cease upon the revocation of the certificate.

(14) The conditions of the ceasing of the service agreement or its termination by extraordinary notice are included in TSP’s GTC.

(15) The TSP shall generate the key pair belonging to the requested certificate by the procedure specified

a\ in Section 6.1 of the Service Practice Statement, and

b\ in the qualified signature creation device (QSCD) specified in Section 6.2 of the same.

(16) Subject data of the requested certificate in accordance with Section 7.1 of the Service Practice Statement:

a\ CountryName: the country of the authority that issued the Client’s identification document

b\ GivenName: given name (first name) part of the Client’s name stated in their personal identification document

c\ SurName: surname (family name) part of the Client’s name stated in their personal identification document

a\ CommonName: full name of the Client as stated in their personal identification document

b\ SerialNumber: unique ID generated by the TSP for the certificate subject

c\ EmailAddress: Client’s e-mail address

(17) The subject data listed in the previous paragraph shall be provided by the Client during the application process, and the TSP shall verify them in accordance with Section 3.2 or 3.3 of the Service Practice Statement.

(18) For the interpretation of the subject data in the certificate see Section 3.1 of the Service Practice Statement.

(19) Other data of the requested certificate:

a\ Validity period (see: Section 6.3.2 of the Service Practice Statement): 1095 calendar days

b\ Liability amount (see: Section 9.2 of the Service Practice Statement): HUF 3,000,000

c\ Certificate Policy (see: Section 1.2.1 of the Service Practice Statement): QCP-n-qscd

d\ Service Component Policy (see: Section 1.2.1 of the Service Practice Statement): EUSCP

(20) In accordance with Section 9.6.1 of the Service Practice Statement, TSP’s liability is to provide the services hereunder in accordance with the Service Practice Statement and the provisions hereof.

(21) In accordance with Section 9.6.3 of the Service Practice Statement Client is obliged:

a\ to provide the TSP with accurate and complete subject data specified in paragraph (16) and other data necessary for his identification during the application for the certificate;

b\ to comply with the restrictions specified in paragraph (8) concerning the use of the certificate and key pair;

c\ to prohibit the unauthorised use of the private key;

d\ to use the private key solely on the cryptographic device specified in paragraph (15), provided by the TSP;

e\ to inform the TSP if the private key or the activation data (password) is compromised in any way (see Section 4.9.12 of the Service Practice Statement).

f\ to inform the TSP of the invalidity or inaccuracy of the data indicated in the certificate;

g\ to terminate the use of the key immediately should the private key or the activation data be compromised in any form;

h\ to terminate the use of the key immediately and permanently should any member of the respective certificate chain become invalid.

(22) Having read and interpreted this agreement Parties have caused it to be duly executed as one fully in accord with their respective intentions.

INDIVIDUAL SERVICE AGREEMENT

For the issuance of Qualified business signing certificate - RQSCD (VideoRA), for rendering related status services as well as for providing and using timestamp, remote key management and signing service

(1) concluded by and between

a\ the Applicant, as the natural person subject of the requested certificate, and also as the natural person acting on behalf of the legal person subject of the requested certificate and the payer of the service fee (hereinafter: Applicant, together Clients)

b\ and NETLOCK Kft. (registered office: H-1101 Budapest, Expo tér 5–7., tax number: 12201521-2-42, website: netlock.hu), as the qualified Trust Service Provider issuing the requested certificate (hereinafter: TSP)

– jointly referred to as Parties – subject to the following terms and conditions.

(2) The issuance of the requested certificate, the remote management of the signature creation data (private key), the use of it within the framework of remote signing service and the related services shall be governed by the documents titled *Service Policy for qualified certificate services* (hereinafter: Service Policy) and the *Service Practice Statement for qualified certificate services* (Service Practice Statement) prevailing at the time of concluding the agreement.

(3) The rendering and use of the qualified timestamp service available within the remote signing service specified in the previous paragraph shall be governed by the document titled *Service Practice Statement for qualified timestamp service* prevailing at the time of concluding the agreement.

(4) The business, legal and technical conditions of concluding the agreement are included in the prevailing version of the General Terms and Conditions (hereinafter: GTC) at the time of concluding the contract, available on the TSP’s website.

(5) The TSP makes a statement about its data processing practice in the Privacy Policy published on its website.

(6) For the information necessary for the Relying Parties during the use of the service see: https://netlock.hu/info/#!/relyingparties

(7) The certificate requested by the Applicant shall be the qualified business signature certificate within the meaning of Section 1.2.1 of the Service Practice Statement.

(8) Pursuant to Section 1.4 of the Service Practice Statement, the requested certificate and key pair belonging to it may be used subject to the following restrictions:

a\ with the private key belonging to the certificate, the Applicant may create a qualified electronic signature in his own name as a natural person cooperating with a legal person certificate Subject;

b\ the certificate and the public key belonging to it may be used for establishing the validity and origin – i.e., the identity of the signatory natural person (Applicant) – of the signatures created by the private key;

c\ the certificate and the key pair belonging to it shall not be used for purposes other than specified above.

(9) In accordance with Section 3.2.1 of the Service Practice Statement, the TSP shall ensure within the framework of the remote key management service that the private key (signature creating data) of the key pair generated for the requested certificate is under the sole control of the Applicant (in his capacity as the natural person Subject of the certificate and as End User) from the moment of its generation until the end of its life cycle.

(10) In accordance with Section 4.1.2 of the Service Practice Statement, the Applicant, as the natural person Subject of the certificate, shall represent as follows:

a\ I have read and accept the GTC, the Service Policy, the Service Practice Statement and the Privacy Policy;

b\ I have read, understand and accept the Clients’ obligations specified in paragraph (21);

c\ I shall use my private key only on the cryptographic device specified in paragraph (15), provided by the TSP;

d\ the natural person subject data specified in paragraph (16) and the other data I have provided during the application for the certificate for the purposes of my identification are true;

e\ I request that the TSP embed my public key generated during the application in the certificate, to certify it and to issue the requested certificate;

f\ I have read and accept the conditions of data processing;

g\ during the validity of the certificate, I shall forthwith inform the TSP of any change in my data stated in the application.

(11) In accordance with Section 4.1.2 of the Service Practice Statement, the Applicant, representing the legal person certificate Subject in this agreement, represents as follows:

a\ I have read and accept the GTC, the Service Policy, the Service Practice Statement and the Privacy Policy;

b\ I have read, understand and accept the Clients’ obligations specified in paragraph (21);

c\ I support the use of the private key (signature creating data) only on the cryptographic device specified in paragraph (15), provided by the TSP;

d\ the legal person Subject data specified in paragraph (16) and the other data I have provided during the application for the certificate for the purposes of identifying the legal person are true;

e\ I have read and accept the conditions of data processing.

(12) In accordance with Section 4.1.2 of the Service Practice Statement, the Applicant, as the natural person representing the Payer of the Service Fee in this agreement, represents as follows:

a\ I have read and accept the selected business conditions;

b\ I undertake to pay the service fee in accordance with the GTC;

c\ I agree to my obligations under paragraph (21);

d\ my fee payer and invoicing data are correct and true;

e\ I have read and accept the conditions of data processing.

(13) Pursuant to Section 4.9 of the Service Practice Statement, the Applicant and the legal person certificate Subject are entitled to apply for the revocation of the requested certificate as follows:

a\ by the Applicant, as End User, electronically, identifying her-/himself in the TSP’s online system; in this case the revocation takes place immediately after the recording thereof in the TSP’s system, within 60 minutes, at the most;

b\ by the Clients by e-mail in the manner specified on the TSP’s website; in this case, the TSP shall perform the revocation within 24 hours from the receipt of the revocation request.

(14) In accordance with Section 4.10 of the Service Practice Statement, the TSP shall provide the related certificate status services (CRL, OCSP) from the issuance of the requested certificate by the end of its validity specified in paragraph (19).

(15) In accordance with Section 4.11 of the Service Practice Statement this agreement

a\ is concluded for a definite period, for the full validity period of the certificate specified in paragraph (19);

b\ shall not cease upon the revocation of the certificate.

(16) The conditions of the ceasing of the service agreement or its termination by extraordinary notice are included in the TSP’s GTC.

(17) The TSP shall generate the key pair belonging to the requested certificate by the procedure specified

a\ in Section 6.1 of the Service Practice Statement, and

b\ in the qualified signature creation device (QSCD) specified in Section 6.2 of the same.

(18) Subject data of the requested certificate in accordance with Section 7.1 of the Service Practice Statement:

a\ CountryName: the country of the legal person certificate Subject’s registered office

b\ GivenName: given name (first name) part of the Applicant’s name stated in their personal identification document

c\ SurName: surname (family name) part of the Applicant’s name stated in their personal identification

document

d\ CommonName: full name of the Applicant as stated in their personal identification document

e\ OrganizationName: full or short name of the legal entity certificate Subject

f\ OrganizationIdentifier: unique ID of the legal entity certificate Subject

g\ SerialNumber: unique ID generated by the TSP for the natural person certificate Subject

h\ EmailAddress: the Applicant’s e-mail address

(19) The subject data listed in the previous paragraph shall be provided by the Applicant during the application process, and the TSP shall verify them in accordance with Section 3.2 or 3.3 of the Service Practice Statement.

(20) For the interpretation of the subject data in the certificate see Section 3.1 of the Service Practice Statement.

(21) Other data of the requested certificate:

a\ Validity period (see: Section 6.3.2 of the Service Practice Statement): 1095 calendar days

b\ Liability amount (see: Section 9.2 of the Service Practice Statement): HUF 3,000,000

c\ Certificate Policy (see: Section 1.2.1 of the Service Practice Statement): QCP-n-qscd

d\ Service Component Policy (see: Section 1.2.1 of the Service Practice Statement): EUSCP

(22) In accordance with Section 9.6.1 of the Service Practice Statement, the TSP’s liability is to provide the services hereunder in accordance with the Service Practice Statement and the provisions hereof.

(23) In accordance with Section 9.6.3 of the Service Practice Statement Clients are obliged:

a\ to provide the TSP with accurate and complete subject data specified in paragraph (16) and other data necessary for her/his identification during the application for the certificate;

b\ to comply with the restrictions specified in paragraph (8) concerning the use of the certificate and key pair;

c\ to prohibit the unauthorised use of the private key;

d\ to use the private key solely on the cryptographic device specified in paragraph (15), provided by the TSP;

e\ to inform the TSP if the private key or the activation data (password) is compromised in any way (see Section 4.9.12 of the Service Practice Statement).

f\ to inform the TSP of the invalidity or inaccuracy of the data indicated in the certificate;

g\ to terminate the use of the key immediately should the private key or the activation data be compromised in any form;

h\ to terminate the use of the key immediately and permanently should any member of the respective certificate chain become invalid.

(24) Having read and interpreted this agreement Parties have caused it to be duly executed as one fully in accord with their respective intentions.

INDIVIDUAL SERVICE AGREEMENT

For the issuance of **Qualified seal certificate - RQSCD (VideoRA)**, for rendering related status services as well as for providing and using timestamp, remote key management and signing service

(1) concluded by and between

a\ the legal person Subject of the requested certificate, also as the payer of the service fee, represented by the Applicant (hereinafter: Client),

b\ and NETLOCK Kft. (registered office: H-1101 Budapest, Expo tér 5–7., tax number: 12201521-2-42, website: netlock.hu), as the qualified Trust Service Provider issuing the requested certificate (hereinafter: TSP)

– jointly referred to as Parties – subject to the following terms and conditions.

(2) The issuance of the requested certificate, the remote management of the seal creation data (private key), the use of it within the framework of remote signature service and the related services shall be governed by the documents titled *Service Policy for qualified certificate services* (hereinafter: Service Policy) and the *Service Practice Statement for qualified certificate services* (Service Practice Statement) prevailing at the time of concluding the agreement.

(3) The rendering and use of the qualified timestamp service available within the remote signature service specified in the previous paragraph shall be governed by the document titled *Service Practice Statement for qualified timestamp service* prevailing at the time of concluding the agreement.

(4) The business, legal and technical conditions of concluding the agreement are included in the prevailing version of the General Terms and Conditions (hereinafter: GTC) at the time of concluding the contract, available on the TSP’s website.

(5) The TSP makes a statement about its data processing practice in the Privacy Policy published on its website.

(6) For the information necessary for the Relying Parties during the use of the service see: https://netlock.hu/info/#!/relyingparties

(7) The certificate requested by the Client shall be the qualified seal certificate within the meaning of the Section 1.2.1 of the Service Practice Statement.

(8) Pursuant to Section 1.4 of the Service Practice Statement, the requested certificate and key pair belonging to it may be used subject to the following restrictions:

a\ with the private key belonging to the certificate, the Applicant, as End User, may create a qualified electronic seal on behalf of the Client;

b\ the certificate and the public key belonging to it may be used for establishing the validity of the seals and the origin – i.e., the identity of the seal user legal person (Client) – of the seals created by the private key;

c\ the certificate and the key pair belonging to it shall not be used for purposes other than specified above.

(9) In accordance with Section 3.2.1 of the Service Practice Statement, the TSP shall ensure within the framework of the remote key management service that the private key (seal creating data) of the key pair generated for the requested certificate is under the sole control of the Applicant representing the Client, in his capacity as End User, from the moment of its generation until the end of its life cycle.

(10) In accordance with Section 4.1.2 of the Service Practice Statement, the Applicant, as the natural person representing the Client, shall declare as follows:

a\ I have read and accept the GTC, the Service Policy, the Service Practice Statement and the Privacy Policy;

b\ I have read, understand and accept the Client’s obligations specified in paragraph (21);

c\ I shall use the private key (seal creating data) only on the cryptographic device specified in paragraph (15), provided by the TSP;

d\ the subject data specified in paragraph (16) and the other data provided during the application for the

certificate for the purposes of identifying the Client and myself are true;

e\ I request that the TSP embed the public key generated during the application in the certificate, to certify it and to issue the requested certificate;

f\ I have read and accept the conditions of data processing;

g\ during the validity of the certificate, I shall forthwith inform the TSP of any change in my data stated in the application;

h\ I have read and accept the selected business conditions;

i\ I agree to my obligations under paragraph (21);

j\ my fee payer and invoicing data are correct and true.

(11) Pursuant to Section 4.9 of the Service Practice Statement, Client is entitled to apply for the revocation of her/his certificate as follows:

a\ electronically, identifying her-/himself in the TSP’s online system; in this case the revocation takes place immediately after the recording thereof in the TSP’s system or within 60 minutes, at the most;

b\ by e-mail in the manner specified on the TSP’s website; in this case, the TSP shall perform the revocation within 24 hours from the receipt of the revocation request.

(12) In accordance with Section 4.10 of the Service Practice Statement, the TSP shall provide the related certificate status services (CRL, OCSP) from the issuance of the requested certificate by the end of its validity specified in paragraph (19).

(13) In accordance with Section 4.11 of the Service Practice Statement this agreement

a\ is concluded for a definite period, for the full validity period of the certificate specified in paragraph (19);

b\ shall not cease upon the cancellation of the certificate.

(14) The conditions of the ceasing of the service agreement or its termination by extraordinary notice are included in the TSP’s GTC.

(15) The TSP shall generate the key pair belonging to the requested certificate by the procedure specified

a\ in Section 6.1 of the Service Practice Statement, and

b\ in the qualified seal creation device (QSCD) specified in Section 6.2 of the same.

(16) Subject data of the requested certificate in accordance with Section 7.1 of the Service Practice Statement:

a\ CountryName: the country of the legal person certificate subject’s registered office

b\ CommonName: the full or short name, DBA name, brand or product name or other name of the legal person certificate subject

c\ OrganizationName: full or short name of the legal person certificate subject

d\ OrganizationIdentifier: unique ID of the legal person certificate subject

e\ EmailAddress: e-mail address of the legal person certificate subject

(17) The subject data listed in the previous paragraph shall be provided by the Applicant during the application process, and the TSP shall verify them in accordance with Section 3.2 or 3.3 of the Service Practice Statement.

(18) For the interpretation of the subject data in the certificate see Section 3.1 of the Service Practice Statement.

(19) Other data of the requested certificate:

a\ Validity period (see: Section 6.3.2 of the Service Practice Statement): 1095 calendar days

b\ Liability amount (see: Section 9.2 of the Service Practice Statement): HUF 3,000,000

c\ Certificate Policy (see: Section 1.2.1 of the Service Practice Statement): QCP-l-qscd

d\ Service Component Policy (see: Section 1.2.1 of the Service Practice Statement): EUSCP

(20) In accordance with Section 9.6.1 of the Service Practice Statement, the TSP’s liability is to provide the services hereunder in accordance with the Service Practice Statement and the provisions hereof.

(21) In accordance with Section 9.6.3 of the Service Practice Statement Client is obliged:

a\ to provide the TSP with accurate and complete subject data specified in paragraph (16) and other data necessary for her/his identification during the application for the certificate;

b\ to comply with the restrictions specified in paragraph (8) concerning the use of the certificate and key pair;

c\ to prohibit the unauthorised use of the private key;

d\ to use the private key solely on the cryptographic device specified in paragraph (15), provided by the TSP;

e\ to inform the TSP if the private key or the activation data (password) is compromised in any way (see Section 4.9.12 of the Service Practice Statement).

f\ to inform the TSP of the invalidity or inaccuracy of the data indicated in the certificate;

g\ to terminate the use of the key immediately should the private key or the activation data be compromised in any form;

h\ to terminate the use of the key immediately and permanently should any member of the respective certificate chain become invalid;

i\ to pay the service fee in accordance with the GTC;

(22) Having read and interpreted this agreement Parties have caused it to be duly executed as one fully in accord with their respective intentions.